UNITED STATES DISTRICT COURT

for the

District of New Hampshire

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Electronic devices located at 659 Marlboro Street, Keene, New Hampshire

Case No. 1-21-mj-72-01-AJ

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see attachment A.

located in the _____ District of New Hampshire, there is now concealed *(identify the person or describe the property to be seized)*:

Please see attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1960, 371	- Prohibition of Unlicensed Money Transmitting Business and Conspiracy
18 U.S.C. § 1001	- False Statements to Federal Government
18 U.S.C. § 1956(a)	- Laundering of Monetary Instruments Including Funds Represented to be Proceeds of Specified Unlawful Activity

The application is based on these facts:

Please see attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Kathryn Thibault
Applicant's signature

Special Agent Kathryn Thibault, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by **Telephonic conference** *(specify reliable electronic means).*

Date: 03/16/2021

Judge's signature

City and state: Concord, New Hampshire

Hon. Andrea K. Johnstone, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Kathryn Thibault, being duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), reporting to the Boston, Massachusetts Division, and have been employed by the FBI since October 1998. I am currently assigned to the Bedford Resident Agency of the FBI and am assigned to work primarily on white collar crime cases. I am familiar with the tactics, methods and techniques of people who commit bank fraud, wire fraud, money laundering and violations of regulations relating to money services businesses. I have attended numerous federal agency and private sponsored training courses. In June 2017, I attended an on-line networking and enterprise training conference in Atlanta, Georgia where cryptocurrency, use of e-mail in money laundering cases and the dark web were topics of instruction. I have participated in financial investigations, and am aware of how targets use the financial system to launder proceeds of illegal activities. As a Special Agent with the FBI, I am responsible for conducting criminal investigations involving violations of Title 18 of the United States Code and other federal statutes enforced by the FBI.

2. In addition, in conducting this investigation and preparing this affidavit, I have consulted with FBI personnel who have substantial expertise investigating crimes involving virtual currency. I have worked closely with FBI analysts who are assigned to FBI Headquarters on the Virtual Currency Evolving Threats (VCET) Team. Specifically, I have worked with two analysts who, as part of their duties at the FBI, have participated in complex international investigations into money laundering facilitators, cyber criminals, national and transnational criminal enterprises, organized crime, and violent crimes. They have extensive experience investigating criminal organizations that leverage virtual assets to launder illicit proceeds, to include violations involving money laundering and operating an unlicensed money transmitting business. Through the course of these investigations, they have advised on investigative strategy, analyzed financial flows, reviewed legal process, and affected virtual asset seizures. They have

also provided training to federal and international law enforcement partners and prosecutorial authorities and participated in numerous virtual currency conferences. Statements in this affidavit regarding virtual currency and the law surrounding virtual currency are based in part on my own knowledge and in part on my conversations and consultation with them.

II. PURPOSE OF THE AFFIDAVIT

3. This affidavit is submitted in support of an application for a search warrant for evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1960, 371 (prohibition of unlicensed money transmitting business and conspiracy), 18 U.S.C. § 1001 (false statements to agent of federal government), 18 U.S.C. § 1956(a) (laundering of monetary instruments, including funds represented to be proceeds of specified unlawful activity), 31 U.S.C. §§ 5313(a) and 5322 (failure to file currency transaction reports ("CTRs")), and 31 U.S.C. § 5318(h) and 5322 (failure to maintain an effective anti-money laundering program) (collectively, the "Subject Offenses"). As set forth below, there is probable cause to search for evidence, contraband, fruits, and instrumentalities of these offenses, as set forth in **ATTACHMENT B** at the premises described in **ATTACHMENT A** (hereby incorporated).

4. On or about March 15, 2021, a federal Grand Jury in the District of New Hampshire returned an indictment charging Ian Freeman ("Freeman"), Colleen Fordham ("Fordham"), Renee Spinella ("R. Spinella"), Andrew Spinella ("A. Spinella"), No First Name Nobody ("Nobody") and Aria DiMezzo ("DiMezzo") with conspiracy to operate an unlicensed money transmitting business in violation of Title 18 United States Code Sections 371, 1960(a), and 1960(b)(1)(B). The indictment charges Freeman, Fordham, R. Spinella, A. Spinella and Nobody with conspiracy to commit wire fraud in violation of Title 18, United States Code, Sections 1343 and 1349 and wire fraud and Freeman with operating a continuing financial crimes enterprise in violation of Title 18 United States Code Section 225 and money laundering in violation of Title 18 United States Code Sections 1956(a)(3)(B). It also charges DiMezzo and Freeman with operating an unlicensed money transmitting business.

5. In addition, on March 15, 2021, United States Magistrate Judge Andrea K. Johnstone issued a warrant authorizing the search of the premises located at 659 Marlboro Street, Keene, New Hampshire, the person of Aria DiMezzo, and any electronic devices in the residence reasonably believed to be used by DiMezzo. *See* Affidavit in Support of Application for Search Warrant, 21-mj-68-01-AJ and 21-mj-65-01-AJ (incorporated herein). I will not set forth all of the facts in that affidavit again but incorporate those facts herein in support of the probable cause with respect to this warrant.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter.

III. PREMISES TO BE SEARCHED

7. This warrant seeks to search electronic devices belonging to or accessible by Michael Horton located in 659 Marlboro Street, Keene, New Hampshire.

IV. BACKGROUND ON VIRTUAL CURRENCY

8. Virtual currency (also known as virtual assets, cryptocurrency, or digital currency, for purposes of this affidavit) is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Examples of cryptocurrency are Bitcoin, Bitcoin Cash, Dash, Monero, and Ether. Virtual currency exists on the Internet, in electronic storage devices, or in cloud-based servers. Virtual currency is not issued by any government, bank, or company and is instead often generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[1] Virtual currency is not illegal in the United States and may be used for legitimate financial

[1] Some cryptocurrencies, like Monero, operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

transactions. However, virtual currency is often used for conducting illegal transactions, such as the sale of controlled substances.

9. Bitcoin is a type of virtual currency. Bitcoin payments are recorded on a public ledger that is maintained by peer-to-peer verification, and is thus not maintained by a single administrator or entity. Individuals can acquire Bitcoins either by "mining" or by purchasing Bitcoins from other individuals. An individual can "mine" for Bitcoins by allowing his/her computing power to verify and record the Bitcoin payments into a public ledger. Individuals are rewarded for this by being given newly created Bitcoins.

10. An individual can send and receive Bitcoins through peer-to-peer digital transactions or by using a third-party broker. Specifically, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Such transactions can be done on any type of computer, including laptop computers and smart phones.

11. Bitcoins are stored in digital "wallets." A digital wallet essentially stores the access code that allows an individual to conduct Bitcoin transactions on the public ledger. To access bitcoins on the public ledger, an individual must use a public address and a private key. The public address can be analogized to an account number while the private key is like the password to access that account. A public address is represented as a case-sensitive string of letters and numbers, 26–35 characters long or a lowercase string of letters and numbers beginning with the prefix "bc1q." Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address. When sending Bitcoin to a public address, an individual may also scan a "QR" code (i.e., a barcode) that contains the address, for easier transmission of that address.

12. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Ledger).

13. Wallets can also be backed up with a "recovery seed," sometimes called a "root key" or "seed key." Recovery seeds are word sequences that represent (encode) a random number used as a seed to derive a wallet. The sequence of words is the wallet backup and can recover and re-create the wallet and all the derived keys in the same or any compatible wallet application.

14. Wallets, represented through recovery seeds and/or private keys, can be backed up into many forms, for example, paper printouts, USB drives, word processing files, or CDs. Additional security safeguards for cryptocurrency wallets can include a complex password and/or two-factor authorization (such as a password and a phrase). Individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

15. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device ("private wallets"). A user typically accesses the private wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the

application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

16. All Bitcoin transactions are recorded on a public ledger known as the "Blockchain," stored on the peer-to-peer network on which the Bitcoin system operates. The Blockchain serves to prevent a user from spending the same Bitcoins more than once. However, the Blockchain only reflects the movement of funds between anonymous Bitcoin addresses and, therefore, cannot by itself be used to determine the identities of the persons involved in the transactions. Only if one knows the identities associated with each Bitcoin address involved in a set of transactions is it possible to meaningfully trace funds through the system.

17. Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are, therefore, described as "pseudonymous," meaning they are partially anonymous.

18. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering, and

is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Dark Web, websites accessible only through encrypted means. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the Dark Web marketplaces. Through the Dark Web or Darknet, i.e., websites accessible only through encrypted means, individuals have established online marketplaces, such as the Silk Road, for narcotics and other illegal items. These markets often only accept payment through virtual currencies, such as Bitcoin. Accordingly, large amounts of Bitcoin sales or purchases by an individual can be an indicator that the individual is involved in narcotics trafficking or the distribution of other illegal items. Individuals intending to purchase illegal items on Silk Road-like websites need to purchase or barter for Bitcoins. Further, individuals who have received Bitcoins as proceeds of illegal sales on Silk Road-like websites need to sell their Bitcoins to convert them to fiat (government-backed) currency.

19. Such illicit purchases and sales are often facilitated by peer-to-peer Bitcoin exchangers, who are not registered with the federal or a state government, or by exchangers that offer a degree of anonymity. These unregistered exchangers often charge a higher transaction fee than legitimate, registered virtual currency exchangers who have robust anti money-laundering programs, including full customer verification.[2] This higher fee is essentially a premium that the unregistered exchangers charge in return for not filing reports on exchanges pursuant to the Bank Secrecy Act, such as Currency Transaction Reports and Suspicious Activity Reports. Peer-to-peer Bitcoin exchangers can conduct these transactions in person or through technology, such as cryptocurrency ATMs (described below).

[2] Based on my training and experience, I am aware that one of the largest U.S.-based (and registered) virtual currency exchanges, Coinbase, charges approximately 2-3% commission per transaction.

V. BACKGROUND ON VIRTUAL CURRENCY AND FINCEN/BSA REGULATIONS

20. Based on my training and experience and the investigation to date, I am aware that exchangers of virtual currency are considered money transmitters under federal law. Specifically, I am aware of the following:

a. The Bank Secrecy Act ("BSA") is codified at 31 U.S.C. §§ 5313-5326. These laws were enacted by Congress to combat the use of financial institutions to launder the proceeds of crime. 31 U.S.C. § 310 establishes the Financial Crimes Enforcement Network ("FinCEN") as a bureau within the Treasury Department, and describes FinCEN's powers and duties to, among other things, enforce compliance with the BSA.

b. The definition of a financial institution under the statute, 31 U.S.C. § 5312(a)(2)(R), includes "a licensed sender of money or any other person who engages as a business in the transmission of funds[.]" Under the relevant federal regulations, financial institutions are also defined as "money servicing businesses," ("MSBs") which include "money transmitters." See 31 C.F.R. § 1010.100(t)(3) (defining "financial institution" as a "money servicing business"); 31 C.F.R. § 1010.100(ff)(5) (defining money transmitters as money services businesses).

c. In 2013, FinCEN issued guidance that a money transmitter can include an individual who offers exchange services between virtual currency and fiat currency. See Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, issued March 18, 2013 (the "FinCEN Guidance"). This guidance was reaffirmed in May 2019. The FinCEN Guidance articulated that those who are money transmitters because they offer exchange services between virtual currency and fiat currency are also MSBs and must comply with the applicable portions of the BSA, some of which are described below.

d. Federal regulations exempt several categories of business and services from the definition of money transmitter, including communication service providers, payment

processors, physical currency transporters (such as armored car services), prepaid access card providers, and individuals who transmit funds integral to the sale of goods or provision of services. 31 C.F.R. § 1010.100(ff)(5)(ii)(A)-(F). None of these exemptions would apply to a digital currency exchanger, such as Freeman and his associates, as described below.

e. Financial institutions, including MSBs and money transmitters, are required to report each deposit, withdrawal, exchange of currency, or other payment or transfer involving more than $10,000 in currency. See 31 C.F.R. §§ 1022.300, 1022.310, 1022.311, and 1022.312 (cross-referencing 31 C.F.R. §§ 1010.300, 1010.310, and 1010.311, and 1010.312); see also 31 U.S.C. § 5313(a). These reports are referred to as Currency Transaction Reports ("CTRs"). A "transaction" for purpose of filing a CTR includes "multiple currency transactions . . . if the financial institution has knowledge that they are by or on behalf of any person and result in either cash in or cash out totaling more than $10,000 during any one business day." 31 C.F.R. § 1010.313. CTRs must be filed within 15 days following the day on which the reportable transactions occurred. See 31 C.F.R. § 1010.306(a)(1). Financial institutions must verify and record the name and address of the individual who conducted the reportable transactions, and must accurately record the identity, social security number, or taxpayer identification number of any person or entity on whose behalf the reportable transaction was conducted. See 31 C.F.R. § 1010.312. CTRs are filed with FinCEN and are made available to law enforcement. It is a federal crime under Title 31 for an MSB or money transmitter to fail to file a CTR. See 31 U.S.C. §§ 5313(a) and 5322.

f. In addition to being required to file CTRs, certain MSBs, including money transmitters, are required to file suspicious activity reports ("SARs"). See 31 C.F.R. §§ 1022.320 (stating at sub-section (a)(1) that money transmitters are a type of MSB required to file SARs). SARs must be filed on transactions aggregating to at least $2,000 in value and the MSB knows or has reason to suspect: (1) the funds are derived from illegal activity or are intended to hide or disguise funds or assets derived from illegal activity to violate or evade any federal law or regulation; (2) the transaction is designed to evade the Title 31 reporting requirements; (3) the

transaction services no apparent business or lawful purpose, and there is no other reasonable explanation for the transaction; and (4) the transaction involves use of the money transmitter to facilitate criminal activity. See 31 C.F.R. §§ 1022.320(a)(2)(i)-(iv). MSBs are required to file a SAR within 30 calendar days after the date of the initial detection of the underlying facts that warrant the filing of a SAR. See 31 C.F.R. §§ 1022.320(b)(3). Lastly, MSBs are required to maintain supporting documentation for the SAR for a period of five years from the date of filing the SAR. See 31 C.F.R. §§ 1022.320(c). It is a federal crime under Title 31 for a money transmitter to fail to file a SAR. See 31 U.S.C. §§ 5318(g) and 5322.

g. Financial institutions, including MSBs and money transmitters, are required to create and maintain effective anti-money laundering compliance programs. See 31 U.S.C. § 5318(h)(1); see also 31 C.F.R. § 1010.210. The program must have written policies, procedures, and controls governing the verification of customer identification, the filing of reports such as CTRs, the creation and retention of records, responses to law enforcement requests, and other compliance with BSA requirements. The anti-money laundering compliance program must have a compliance officer who is responsible for assuring that the business complies with all BSA requirements. It is a federal crime under Title 31 for an MSB or money transmitter to fail to maintain an effective anti-money laundering compliance program. See 31 U.S.C. §§ 5318(h)(1) and 5322.

h. Any person who owns or controls an MSB is responsible for registering, and periodically re-registering, the business with FinCEN. See, 31 U.S.C. § 5330(a); see also 31 C.F.R. § 1022.380. Registration must be done on or before the end of the 180-day period beginning on the day following the date the business was established. See, 31 C.F.R. § 1022.380(b)(3). A money transmitting business that fails to register with FinCEN is subject to criminal liability under 18 U.S.C. § 1960. Specifically, § 1960 makes criminally liable anyone who "knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business." That includes, under 18 U.S.C. § 1960(b)(1)(B), a business that "fails to comply with the money transmitting business registration requirements

under section 5330 of title 31, United States Code, or regulations prescribed under such section[.]"

i. Additionally, even if a money transmitter is registered with FinCEN, 18 U.S.C. § 1960(b)(1)(C) also criminalizes money transmitting businesses that "involve . . . the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity."

VI. BACKGROUND ON CRYPTOCURRENCY AUTOMATED TELLER MACHINES

21. Based on my training and experience, I am aware of the following.

22. Cryptocurrency ATMs are electronic terminals that act as mechanical agencies of the owner-operator, to enable the owner-operator to facilitate the exchange of cryptocurrency for currency or other cryptocurrency. Many types of cryptocurrencies may be purchased through cryptocurrency ATMs (and in fact the ATMs discussed in this warrant sell different types of cryptocurrencies including Bitcoin, Bitcoin Cash, Dash and Monero). These cryptocurrency ATMs may connect directly to a separate exchanger, which performs the actual cryptocurrency transmission, or they may draw upon the cryptocurrency in the possession of the owner-operator of the electronic terminal. In this investigation, Freeman used his own cryptocurrency accounts to provide exchange services. Thus, a transactor at the ATM need not have an account with Freeman or any connection to Freeman in order to obtain or sell cryptocurrency.

23. Under FinCEN's guidance (FIN-2019-G001, May 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf), an owner-operator of a cryptocurrency ATM who uses an electronic terminal to accept currency from a customer and transmit the equivalent value in cryptocurrency (or vice versa) qualifies as a money transmitter both for transactions receiving and dispensing currency.

24. Cryptocurrency ATMs often look like traditional banking ATMs and can contain some of the same physical features as a regular bank ATM such as: a touch screen, keypad, cash

dispenser, receipt printer, cash and/or card reader, and are generally free-standing machines. These features allow crypto ATMs to accept cash for payment, in exchange for cryptocurrency, which is transferred to the cryptocurrency address of the user's choice. The kiosk generally gives a paper receipt that contains the details of the transfer. Cryptocurrency ATMs can also take cryptocurrency and provide a user with cash, but I believe this feature has been disabled on the ATMs at issue in this case.

25. Cryptocurrency ATMs are secured with external locks to both the machine itself and to the internal cash boxes. Inside the ATM is usually a built-in computer system or digital tablet configured to run software to facilitate transactions. The hardware and software maintain computer logs, like any regular computer or tablet, related to the operating system, software applications, and transactional data. Cryptocurrency ATMs allow the owner/operator to attach a keyboard to the computer or tablet to interact with the operating system and software for administrative purposes.

V. SUMMARY OF PROBABLE CAUSE

26. In 2017, the FBI, Internal Revenue Service ("IRS"), and the United States Postal Inspection Service ("USPIS") initiated an investigation of Freeman and his associates and their virtual currency-fiat cash exchange business. The investigation has revealed that since at least 2015, Freeman has operated an unlawful money services business ("MSB") selling millions of dollars in virtual currency. By operating an unlicensed MSB, Freeman sells virtual currency without abiding by any FinCEN and Bank Secrecy Act regulations which require MSBs to, among other things, have an anti-money laundering program, file SARs and CTRs, and collect know-your-customer information. Freeman runs his business through purported religious organizations that he and his co-conspirators have founded including the Shire Free Church, the Crypto Church of NH, the Church of the Invisible Hand, the NH Peace Church, and the Reformed Satanic Church. In order to mislead banking institutions and prevent them from identifying the business as an MSB, Freeman and his co-conspirators engage in a series of lies and omissions, most commonly describing deposits into bank accounts for virtual currency

purchases as "church donations" and transfers of money to buy virtual currency as "church outreach." Freeman also uses personal bank accounts to run his business and instructs co-conspirators to open bank accounts in their names for his use.

27. Freeman and others sell virtual currency in two ways. They advertise on peer-to-peer virtual currency trading websites, such as LocalBitcoins.com ("LBC") and Paxful.com, where they accept bank deposits, wires, or cash sent by mail in exchange for cryptocurrency.[3] They also operate various cryptocurrency ATMs. Freeman generally charges a 5% to 15% or higher fee for transactions – which is significantly higher than what a customer is charged by a regulated virtual currency exchange that complies with U.S. anti-money laundering laws, such as Coinbase. As of March 6, 2021, FinCEN records confirmed that Freeman, his co-conspirators, and the entities they operate have not registered with FinCEN as an MSB in violation of 18 U.S.C. § 1960(b)(1)(B).

28. Freeman is very careful about making clear that virtual currency clients should not tell him what they do with their money. In fact, on the ATMs, he posted instructions which clearly state, "do not tell our staff why you want the coins" and on his LBC profile he wrote, "what you do with your bitcoin is your business. Don't tell me what your plans are. If you do, I reserve the right to refuse the sale." Nevertheless, law enforcement has learned that criminal actors who use virtual currency to further their crimes have successfully exploited Freeman's business for separate criminal pursuits, often involving online scams and fraud. Please reference incorporated affidavit for additional facts relating to this investigation.

VI. MICHAEL HAMPTON

29. On March 16, 2016, law enforcement agents executed a search warrant at the Subject Premises. That warrant authorized the search and seizure of devices used by Aria DiMezzo only. While searching the premises, officers encountered Michael Hampton who lives

[3] Localbitcoins.com is a peer to peer Bitcoin exchange. It is an online marketplace where individuals can buy, sell and trade Bitcoin with each other. The site allows users to post advertisements where they state exchange rates and payment methods for buying or selling bitcoins. The advertisements allow clients to reply to these advertisements and agree to meet in person to buy bitcoins with cash, or trade directly with online banking. I know that Paxful is a global cryptocurrency trading platform that operates like localbitcoins.com.

in the residence. SA Ryan Burke who was present at the search warrant relayed the following information to me.

30. The FBI conducted a consensual interview of Hampton. Hampton said that he is friends with DiMezzo and Freeman. He said that he is aware that Freeman operates bitcoin ATMs and transacts in bitcoin but that he was not personally involved in Freeman's business. He believed that the Shire Free Church was the name of Ian's business. He stated that he hosts a radio show with Freeman and that Freeman pays him $20 in bitcoin per show. He also stated that he has cancer and that Freeman posted his story online, generating donations in bitcoin from various people.

31. Hampton told officers that he used to have a lot of bitcoin but he spent most of it and only has a small amount left. Hampton signed a written consent form allowing FBI agents to search his telephone and provided them with the passwords for the phone. While reviewing that telephone, agents observed a conversation on Telegram (an encrypted messaging platform) entitled "Keene Chat." At 6:08 a.m. this morning, Hampton wrote to the chat "FBI hrte" and someone responded, "ohh shit" and "should we come?" Other group members than began to send photographs of FBI vehicles to the chat.

32. Upon further review of the telephone, agents found that there was frequent communications with Freeman about the bitcoin ATMs and it appeared that Hampton had responsibility for maintenance or technical support for the ATM machines and related servers. On March 10, 2021, Freeman sent Hampton a message telling him that he was dropping off some disk drives to the Subject Premises. Hampton then replied to Freeman providing him with the code for the door lock at the Subject Premises.

33. Agents confirmed that various emails recovered in search warrants indicated that Freeman employed a "Michael" to service and provide technical support for his bitcoin ATMs. For example, on January 15, 2016, a "Michael" using email address bvm5ne@gmail.com contacted the ATM manufacturer and wrote, "I'm working for Ian Freeman on the machine we just received in New Hampshire" and then listed various technical issues with the machine. In

another email sent in 2017, Freeman referred to Michael as his "technical admin." In that series of emails, Michael had reached out to a company called Breadwallet about a problem that a bitcoin customer had at the ATM. I believe that Michael the technical admin is Michael Hampton. I also believe that Hampton lied to investigators when he said he was not involved in Freeman's bitcoin business.

34. Hampton said he repairs laptops and sells them on eBay. In his bedroom, SA Burke observed a desktop computer tower, a MacBook which Hampton said he used yesterday, various other laptops (at least 5) and various hard drives (at least 6) among other devices.

35. Although Hampton gave officers consent to search his phone he would not give consent to search the computer in his room. He said it was used primarily for gaming and pornography. I believe, however, that the electronic devices may have evidence of the unlawful ATM business conducted by Freeman and others. I also seek authority to search his phone and other devices found in the room for evidence of the scheme. I also believe that these devices will contain evidence of the fact that Hampton's statements to federal agents about his involvement in the business were false.

36. Freeman's ATMs are manufactured by GeneralBytes. GeneralBytes provides the ability for cryptocurrency ATM operators, such as Freeman, to use on servers that the operator maintains. In an April 2018 email exchange with GeneralBytes, Freeman said that he would operate the ATMs from his own server that he runs. Information on this server may be accessible from Hampton's devices.

37. I know that people who engage in financial crimes like operating an unlicensed money transmitting business and wire fraud often save bank and financial records for many years and that they often save these records in electronic devices in their residences especially when they operate the businesses from their residences. The financial crimes these individuals are charged with began in 2015 and I believe that financial records dating back to that year may be kept on the devices to be searched. I also believe that people general keep financial documents,

money, cash equivalents, and other proceeds of these unlawful schemes for long periods of time on their devices.

38. Individuals involved in digital currency use a variety of digital devices, such as phones and computers. These individuals use multiple digital devices in order to maintain anonymity and to compartmentalize communication, or use encrypted forms of communication in speaking with criminal associates like Hampton and Freeman's use of Telegram. Additionally, those who use digital currency may store their recovery key or private keys on digital devices, to include phones, computers, laptops, tablets, and hardware wallets. Based on my training and experience, I know that any individual, to include co-conspirators, with access to a cryptocurrency wallet's recovery key or private keys has the means to transfer the corresponding cryptocurrency held in that wallet. This can be done very quickly.

39. People may also store financial records, photos and videos of co-conspirators or depicting expenditures of money or criminal conduct, contact lists, chats, and other records on digital devices. This also includes personal digital devices that the individual carries on their person. I believe that people who use virtual currency to conduct exchanges on the dark web do so using cell phones and computers.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

40. Based on my training and experience, I am aware that businesses frequently use computers to carry out, communicate about, and store records about their business operations. These tasks are frequently accomplished through sending and receiving business-related email and instant messages; drafting other business documents such as spreadsheets and presentations; scheduling business activities; arranging for business travel; storing pictures related to business activities; purchasing and selling supplies online; researching online; and accessing banking, financial, investment, utility, and other accounts concerning the movement and payment of money online. From my training and experience I know that many smartphones can now function essentially as small computers. They have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving

text messages and emails, conducting financial activities and storing a vast amount of electronic data.

41. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled

environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.[4] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve

[4] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular

use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

42. I also know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-

recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

43. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

44. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall

2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

45. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

46. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

47. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a

certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

48. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features (such as with Touch ID devices, which can be registered with up to five fingerprints), and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device.

49. For these reasons, if while executing the warrant at Subject Premises, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to Hampton, during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is (a) located

at the place searched and (b) falls within the scope of the warrant: (1) compel the use of the person's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

50. The proposed warrant does not authorize law enforcement to compel that an individual present at the Subject Premises state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel an individual present at the Subject Premises to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Devices.

VIII. CONCLUSION

51. For all the reasons described above, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 1960, 371 (prohibition of unlicensed money transmitting business and conspiracy), 18 U.S.C. § 1001 (false statements to agent of federal government), 18 U.S.C. § 1956(a) (laundering of monetary instruments, including funds represented to be proceeds of specified unlawful activity), 31 U.S.C. §§ 5313(a) and 5322 (failure to file currency transaction reports ("CTRs")), and 31 U.S.C. § 5318(h) and 5322 (failure to maintain an effective anti-money laundering program) (collectively, the "Subject Offenses"), as described above in Attachments B-1 through B-15 of this affidavit will be found in a search of **SUBJECT PREMISES A-1 through A-15** as further described above and in Attachments A-1 to A-15 of this affidavit.

Respectfully Submitted,

/s/ Kathryn Thibault
Kathryn Thibault
Special Agent, Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Mar 16, 2021
Time: 11:45 AM, Mar 16, 2021

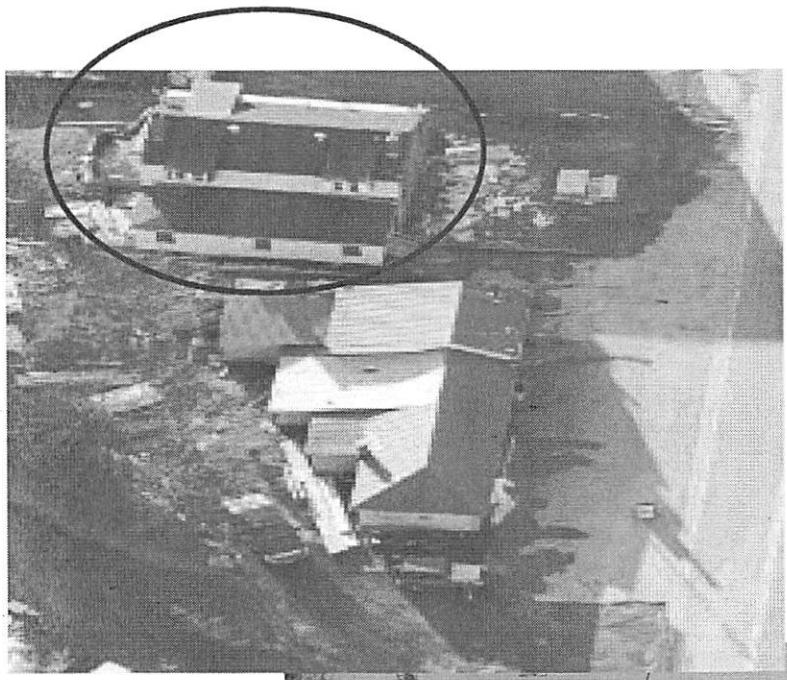
HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

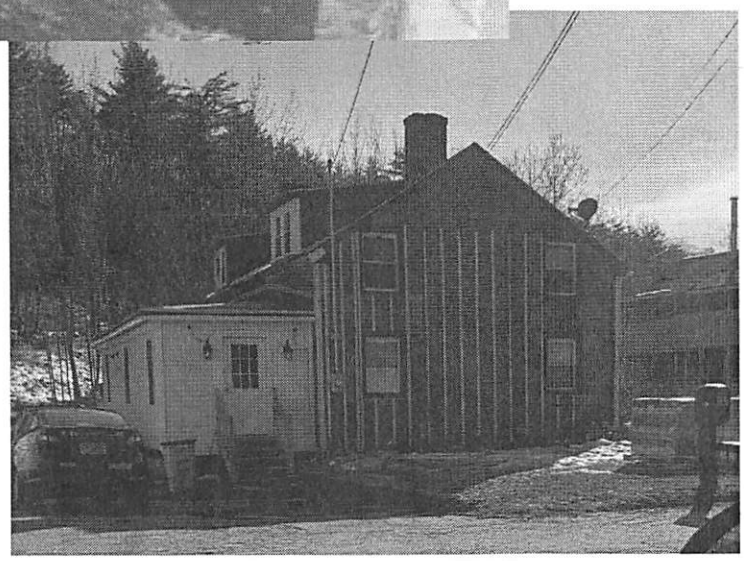
ATTACHMENT A

Electronic Devices used and accessed by Michael Hampton located in 659 Marlboro Street, Keene, New Hampshire

The Subject Premises is a two story red brick residence with a one level white panel siding addition located on the left side of the brick structure. The front door to the residence is located on the left side of the structure. The front door is located at the end of the driveway with two porch lights on either side of the door. The two story red brick portion of the residence sits to the right of the front door and has two windows on the first floor and two on the second floor facing Marlboro Street. The only parking for the residence is in the driveway on the left side of the property which ends at the front door entrance.

The warrant seeks authority to seize and search electronic devices used and accessed by Michael Hampton found in the residence.





ATTACHMENT B-

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 1960, 371 (prohibition of unlicensed money transmitting business and conspiracy), 18 U.S.C. § 1001 (false statements to agent of federal government), 18 U.S.C. § 1956(a) (laundering of monetary instruments, including funds represented to be proceeds of specified unlawful activity), 31 U.S.C. §§ 5313(a) and 5322 (failure to file currency transaction reports ("CTRs")), and 31 U.S.C. § 5318(h) and 5322 (failure to maintain an effective anti-money laundering program) (collectively, the "Subject Offenses"), namely:

a. Indicia of occupancy, residency, and/or ownership of the previously described property, including utility and telephone bills, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, envelopes, registration, receipts, and keys which tend to show the identities of the occupants, residents, and/or owners.

b. Any digital device, including devices containing cryptocurrency, which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof, reasonably believed to be used or accessed by Michael Hampton.

c. For any computer, computer hard drive, or other physical object upon which electronic data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant.

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious

software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment;

j. evidence of the crimes described above in paragraph 1 including but not limited to evidence regarding bitcoin ATMs and their servers, Hampton's role in the bitcoin ATM business, conversations with Ian Freeman and other co-conspirators, discussions of bitcoin, financial records, virtual currency, communications regarding virtual currency, evidence of the location and access to virtual currency, evidence of the expenditure of assets, evidence of use of the dark web, records of operations of cryptocurrency ATMs, records of knowledge of FinCEN reporting requirements, the text messaging application Telegram and included communications regarding cryptocurrency, use of peer-to-peer cryptocurrency exchanges, internet search results relating to the crimes herein, evidence of Hampton's knowledge of and role in Freeman's business and the veracity of his statements to the FBI, records and things

evidencing the use of the Internet, including: records of Internet Protocol addresses used; records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

DEVICE UNLOCK: During the execution of the search of the property described in Attachment A, and with respect to any device at/on SUBJECT PREMISES reasonably believed to be owned, used, or accessed by Michael Hampton, law enforcement personnel are authorized to (1) compel the use of the person's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

As used above, the term "COMPUTER" includes but is not limited to any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, thumb drives, flash drives, Micro SD cards, SD cards, CDs, DVDs, tape drives and tapes, optical storage devices, zip drives and zip disk media, and other memory storage devices);

peripheral input/output devices (such as keyboards, printers, fax machines, digital cameras, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, routers, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).